Securitas

2025

Informe de Perspectivas Tecnológicas Globales

Bienvenidos a nuestro Informe de Perspectivas Tecnológicas Globales 2025

En Securitas nos complace presentar la edición 2025 de nuestro tan esperado Informe de Perspectivas Tecnológicas Globales. En su séptimo año, el informe contiene abundante información basada en datos sobre el futuro de la tecnología de la seguridad y las empresas de todo el mundo que la desarrollan.

Como reflejo de nuestra pasión por la orientación al cliente, la innovación tecnológica y la excelencia operativa, el contenido de este informe está pensado para ayudarte a conocer las nuevas tendencias de la seguridad electrónica y evaluar cómo aprovechar el potencial de las tecnologías emergentes para tu empresa.

Este año, el informe se centra en los principales temas de actualidad que marcarán el sector de la seguridad en 2025. Entre otros, inteligencia artificial (IA) y análisis de datos, tecnología en la nube, ciberseguridad y protección de datos, tecnologías emergentes y sostenibilidad.

Comprender cómo aprovechan las empresas estas tendencias es fundamental a la hora de considerar la hoja de ruta tecnológica y las inversiones futuras. Es precisamente por ello por lo que nuestro apartado de perspectivas se ha convertido en una parte clave del informe para nuestros clientes, ya que presenta información sobre los principales fabricantes de productos y tecnólogos del sector, así como del mercado, incluidos datos de encuestas exclusivas sobre adopción de tecnología, implantación e inversiones futuras compartidos por los responsables de seguridad electrónica de más de 1.000 empresas de todo el mundo.

La elaboración de este informe no hubiera sido posible sin nuestro conocimiento del mercado y el apoyo incondicional de varios colaboradores importantes, especialmente de nuestros socios tecnológicos estratégicos y del Consejo Asesor de Clientes. Su sólida experiencia, perspectiva única y valiosos conocimientos, junto con su colaboración activa con nuestro equipo de Estrategia e Innovación Tecnológica, nos ofrecen una visión clave sobre la evolución de la innovación tecnológica en seguridad, tanto en el presente como en el futuro.

Por último, nos gustaría darles las gracias por dedicar su tiempo a leer este informe. La tecnología de seguridad sigue evolucionando a un ritmo vertiginoso y estamos comprometidos con mantener informados a nuestros clientes sobre lo que está por venir. Gracias a nuestra presencia global, operaciones locales, sistemas escalables, servicios personalizados a un enfoque centrado en la excelencia operativa, gozamos de una posición única para ser el mejor socio tecnológico del sector. Agradecemos profundamente la oportunidad de ser tu asesor de confianza y asumimos esta responsabilidad con la máxima seriedad.

Tony Byerly
Global President
Securitas Technology, Securitas AB
& Chief Executive Officer
Securitas Technology Corporation


Pb

Índice

Perspectivas

Trending Topics

Perspectivas del mercado

Hemos encuestado a más de 1.000 personas con capacidad de decisión en materia de seguridad electrónica y responsables de la supervisión de la implantación de sistemas de seguridad y programas de seguridad electrónica en todo el mundo. El estudio tiene como objetivo analizar la forma en la que las empresas aprovechan los sistemas, los servicios y la tecnología de seguridad para afrontar los riesgos emergentes, mitigar amenazas y mejorar la eficiencia operativa. Nuestra investigación abarca cinco temas principales: tecnologías emergentes, soluciones en la nube, ciberseguridad y protección de datos, inteligencia artificial y análisis de datos, y sostenibilidad. **Esto proporciona una información muy valiosa** para que las empresas puedan evaluar sus estrategias a la luz de las normas del sector y descubrir enfoques innovadores utilizando las tecnologías de seguridad para obtener una ventaja competitiva.

A lo largo de este informe, hacemos referencia a datos recopilados en una encuesta realizada para Securitas Technology en 2024 por una empresa externa de estudios de mercado. En la encuesta participaron 1.100 encuestados de Australia, Francia, Alemania, Reino Unido y Estados Unidos. Entre los participantes se encontraban personas de organizaciones comerciales e industriales de diferentes sectores que eran los principales responsables o que tenían una influencia significativa en las decisiones relacionadas con las inversiones en seguridad electrónica y también responsables de la implantación de sistemas de seguridad electrónica en su organización. Estos usuarios finales fueron identificados de forma independiente por la empresa de estudios de mercado externa y pueden ser o no socios comerciales de Securitas Technology.

Datos, tendencias y perspectivas

Tecnologías de seguridad electrónica tradicionales más adoptadas en la actualidad.

1. Videovigilancia
2. Detección de incendios
3. Control de accesos

Las 3 amenazas principales para la seguridad que impulsan e influyen en el uso de la seguridad electrónica.

1. Ciberseguridad
2. Robo externo e interno
3. Intrusión y merodeo

El **61%** de los que aún no utilizan la monitorización remota de alarmas está interesado en hacerlo en los próximos 18 meses.

Principales servicios basados en suscripción implantados en las empresas.

1. Monitorización de alarmas
2. Protección contra incendios y prevención de emergencias.
3. Portales de gestión de seguridad
4. Servicios en la nube

El **85%** de las empresas encuestadas consideró la sostenibilidad como un factor importante o muy importante a la hora de elegir la tecnología de seguridad.

Principales tecnologías de seguridad emergentes.

	La uso actualmente	No la uso pero me interesaría usarla
Servicios en la nube	58%	52%
Inteligencia artificial	46%	45%
Tecnología adaptativa	46%	39%
Análisis predictivo	39%	46%

Las 5 tecnologías principales basadas en inteligencia artificial y análisis de datos en el campo de la seguridad electrónica que las empresas están más interesadas en explorar en los próximos 12 meses...

1. Detección de intrusiones - **63%**
2. Reconocimiento facial - **56%**
3. Detección de anomalías - **48%**
4. Reconocimiento de matrículas - **48%**
5. Detección de vehículos - **44%**

Uso actual en las empresas de los datos de las tecnologías de seguridad electrónica.

46% para mejorar la experiencia de los empleados y clientes.

45% para aumentar la eficiencia operativa y reducir los costes

39% para apoyar las operaciones y equipos de vigilancia física

A medida que se recopilan y utilizan más datos sobre seguridad electrónica, **la ciberseguridad y el cumplimiento de la legislación sobre protección de datos y confidencialidad se tienen más en cuenta en las decisiones de contratación y** gestión.

Datos procedentes de una encuesta externa realizada por Securitas Technology, en la que participaron 1.100 responsables de la toma de decisiones sobre seguridad y de la implantación de sistemas de seguridad de diferentes sectores en Australia, Francia, Alemania, Reino Unido y Estados Unidos.

1 Trending Topics

Tecnologías emergentes

Las tecnologías emergentes siguen aportando nuevas e interesantes innovaciones al sector de la seguridad electrónica.

Desde la videovigilancia con inteligencia artificial (IA) incorporada, hasta los sistemas de control de accesos biométrico sin contacto, las soluciones de última generación permiten a las empresas simplificar la gestión de sus sistemas, mejorar su seguridad y adoptar las tecnologías más avanzadas en protección.

En este apartado, analizaremos la forma en la que las empresas y sus proveedores de servicios pueden hacer uso de algunas de estas tecnologías nuevas y emergentes para mejorar la eficiencia de las soluciones de seguridad electrónica y los servicios de asistencia.

Las 3 principales tecnologías:

- Servicios en la nube
- Inteligencia artificial
- Análisis predictivo

que las empresas están más interesadas en adoptar en los próximos 18 meses.

El **31%** utiliza la biometría sin contacto.

El **42%** de las que aún no la utilizan, están interesadas en usarla en los próximos 18 meses.

El **39%** cree que las preocupaciones sobre la protección de datos y el cumplimiento normativo limitan el uso de las tecnologías de seguridad electrónica emergentes.

Datos procedentes de una encuesta externa realizada por Securitas Technology, en la que participaron 1.100 responsables de la toma de decisiones sobre seguridad y de la implantación de sistemas de seguridad de diferentes sectores en Australia, Francia, Alemania, Reino Unido y Estados Unidos.

Aprovechar el potencial de las tecnologías emergentes para mejorar la seguridad electrónica

Alertas por excepción con analítica de borde

La tecnología de videovigilancia mejorada con funciones de análisis de datos es cada vez más potente y asequible, lo que permite a las empresas utilizar sus cámaras de seguridad para prevenir incidentes en lugar de grabarlos simplemente. Históricamente, el hardware de seguridad siempre se ha desarrollado de manera más lenta respecto al software de procesamiento de datos que lo respalda. Por ello, para aprovechar los beneficios del análisis de vídeo inteligente, las empresas necesitaban un ancho de banda considerable, servidores costosos y unidades de procesamiento gráfico (GPU). Ahora, esto ha cambiado gracias a la mayor disponibilidad y al menor coste de los microchips de última generación que utilizan las cámaras de seguridad para procesar datos.

La evolución de la analítica de borde (en el que las cámaras están equipadas para poder procesar grandes cantidades de datos por sí mismas o en "el borde") ha ampliado la posibilidad de que las empresas superpongan análisis inteligentes con algoritmos de inteligencia artificial (IA) a su red de seguridad. Esto se debe a que la tecnología inteligente que incorpora la cámara de borde permite capturar, procesar y analizar datos dentro del dispositivo, sin necesidad de enviar todos esos datos a un servidor central. De este modo, solo es necesario enviar el resultado del análisis, lo que reduce considerablemente el ancho de banda y elimina por completo la necesidad de un servidor central potente.

Las cámaras de borde con análisis de vídeo y audio incorporado se pueden programar para comprender su entorno, reconocer patrones normales de actividad, escuchar sonidos hostiles e identificar personas y vehículos atendiendo a diferentes características. Sobre la base de estos datos, las cámaras pueden alertar sobre actividades y sonidos sospechosos o que difieren del comportamiento esperado. Por ejemplo, pueden detectar agresiones, disparos, merodeos, seguimientos de cerca y entradas en escena de objetos, personas y vehículos desconocidos que podrían representar amenazas potenciales. Este enfoque proactivo ayuda a reducir las falsas alarmas y facilita una respuesta más rápida de los operadores de seguimiento remoto, quienes pueden verificar las amenazas auténticas y activar la megafonía local para advertir a los intrusos antes de que los incidentes se agraven aún más.

Búsqueda de sencillez y eficacia con la gestión en el móvil

Supervisar tareas importantes sobre la marcha es más fácil cuando se tiene acceso a toda la información en la palma de la mano. Esta es una de las principales innovaciones del sector, que incluye aplicaciones móviles intuitivas (apps) que ayudan a los responsables de seguridad y propietarios de empresas a controlar y hacer un seguimiento de sus sistemas de seguridad de control de accesos, videovigilancia e intrusión de forma remota.

Utilizando el acceso remoto a las tecnologías de seguridad a través de aplicaciones, las empresas pueden gestionar su seguridad de forma más eficaz,

desde cualquier lugar del mundo y a cualquier hora del día. Ya sea que deseen revisar la actividad en un lugar determinado o administrar cambios en un sistema específico, la gestión móvil ofrece a los usuarios una visión simplificada incluso del programa de seguridad más complejo, además de poner a su disposición funciones como:

- Notificaciones de alarma instantáneas.
- Retransmisiones de vídeo en directo y grabado.
- Control remoto del sistema mediante teclados virtuales.
- Acceso a informes del sistema, historial de eventos y registros de actividad.
- Administración de usuarios y gestión de credenciales.

La necesidad de eficiencia operativa significa que ahora los clientes esperan tener acceso a aplicaciones móviles y de escritorio cuando instalan o actualizan sus sistemas de seguridad. Estas aplicaciones ofrecen información clave sobre la actividad diaria del sistema y del emplazamiento, como informes de armado y desarmado y visibilidad del horario y presencia de los empleados. A medida que crece la demanda de tecnología basada en la nube, los desarrolladores de productos seguirán haciendo grandes inversiones en nuevas características móviles e innovaciones fáciles de usar para diferenciar sus soluciones en un entorno cada vez más saturado.

Reinventar la gestión de la identidad mediante la biometría sin contacto

El control de accesos biométrico sigue siendo el método más avanzado de gestión de identidades que existe en la actualidad en aquellos países cuya normativa permite su utilización. La singularidad de las características biológicas, como las huellas dactilares y los rasgos faciales, las convierte de forma natural en credenciales ideales para aplicaciones de seguridad, ya que ofrecen mayores niveles de autenticación en comparación con los métodos de acceso electrónico más utilizados, como códigos clave, tarjetas inteligentes y credenciales móviles.

En 2025 se cumplen cinco años desde que la pandemia del coronavirus (COVID-19) causó un gran impacto en todo el mundo y representó una amenaza significativa para la salud de la población mundial. El aumento de la importancia de las medidas de higiene (para ayudar a minimizar la propagación del virus) intensificó la necesidad de soluciones de acceso sin contacto/sin fricción que pudieran ayudar a reducir el riesgo de contaminación cruzada y de propagación del virus, manteniendo al mismo tiempo altos estándares de gestión segura de identidades. Esto no hizo más que reforzar los beneficios de la biometría como la solución de control de accesos más segura e higiénica, impulsando una mayor inversión en este apasionante campo de la tecnología, tanto por parte de innovadores de productos como de empresas usuarias finales.

Si bien el reconocimiento de las huellas dactilares, facial, del iris y de la palma de la mano ya se han

"La IA y la nube están ampliando los límites de la seguridad electrónica e influyen en nuestros socios tecnológicos a la hora de desarrollar soluciones más inteligentes y preparadas para el futuro. Nos centramos en el valor tangible que pueden aportar estas innovaciones, comprometiéndonos a ayudar a nuestros clientes a adoptar nuevas características y funciones."

Sabrina Stainburn | President, Europe | Securitas Technology

consolidado como credenciales de control de accesos biométrico, junto con la difusión de la IA y el reforzamiento de la normativa sobre protección de datos, estamos viendo un **interés cada vez mayor en el mercado por la biometría sin contacto. Nuestro Consejo Asesor de Clientes lo ha comprobado y la mayoría de sus miembros son "favorables" o "muy favorables" a utilizar lectores biométricos sin contacto en la empresa.**

Una forma particular de biometría cada vez más popular es la tecnología de identificación facial. Con la instalación de terminales de reconocimiento facial en puntos de acceso clave se puede lograr una mayor eficiencia operativa y una reducción de costes, así como una mayor comodidad para empleados y visitantes y menores tiempos de espera. Además, ya no es necesario adquirir, emitir ni reemplazar tarjetas o tokens de acceso físicos redundantes. Una vez que se ha registrado un rostro en el sistema de control de accesos, el reconocimiento facial también se puede integrar con otras aplicaciones, incluido el control de horario y presencia. A medida que el reconocimiento facial vaya siendo más habitual, creemos que la biometría de reconocimiento de voz se convertirá en una tecnología a tener en cuenta en los próximos años.

Transformación de los servicios de asistencia con realidad virtual y aumentada

La realidad virtual (RV) y la realidad aumentada (RA) ocupan los primeros puestos de la lista de tecnologías emergentes que las empresas explorarán en 2025. Creemos que esta tendencia seguirá generando nuevos usos dentro del mundo de la seguridad, especialmente cuando se trata de mejorar la experiencia del cliente. Los proveedores de servicios de seguridad ya están aprovechando estas tecnologías para impulsar la próxima generación de servicios y asistencia.

Por ejemplo, los técnicos de asistencia in situ pueden usar dispositivos de RA para superponer esquemas a equipos en el mundo real, lo que permite realizar reparaciones más rápidas y eficientes. Las aplicaciones que incorporan la RA también pueden permitir que personal capacitado de asistencia técnica remota solucione problemas, diagnostique y repare averías de manera efectiva sin necesidad de acudir en persona, lo que minimiza las interrupciones, los costes y el impacto medioambiental. Y, apoyándose en la realidad virtual, los clientes pueden realizar simulacros de seguridad virtuales, mientras que los proveedores de servicios pueden ofrecer formación técnica inmersiva.

A medida que el sector de la seguridad va evolucionando y surgen tecnologías modernas, las posibilidades parecen infinitas tanto para los clientes como para los proveedores de servicios. Ahora, las empresas tienen que revisar continuamente la escalabilidad de su programa de seguridad y analizar cómo pueden contribuir las nuevas tendencias y características tecnológicas a lograr una mayor eficacia en el futuro.

"Las tecnologías emergentes están dando lugar a nuevas formas de pensar en la prestación de servicios. Tomemos como ejemplo la realidad virtual y aumentada; el potencial que ofrece el aprovechamiento de estas herramientas para ayudar a mejorar la experiencia de nuestros clientes es realmente interesante y un aspecto clave dentro de nuestra estrategia de innovación tecnológica."

Kevin Engelhardt | President, North America | Securitas Technology

2 Trending Topics

Inteligencia artificial y análisis de datos

La presencia de la Inteligencia Artificial (IA) y el análisis de datos en el sector de la seguridad electrónica sigue despertando interés y generando innovación. Sin embargo, la percepción de estas tecnologías, sus beneficios y el papel que desempeñan junto a las personas está en constante cambio.

Sabemos a través de nuestro Consejo Asesor de Clientes que las empresas están apreciando el valor de la IA. Pero ¿cómo pueden encontrar el equilibrio adecuado entre la IA y la experiencia humana dentro de su programa de seguridad? ¿Y cómo pueden beneficiarse los responsables de seguridad con el uso de esta nueva generación de datos? Estas son las preguntas clave que vamos a abordar en este apartado.

En esta sección exploramos la influencia creciente de la IA en la innovación de la tecnología de seguridad y analizamos cómo pueden aprovechar las empresas los conocimientos basados en datos para contribuir a mejorar la protección de su negocio y complementar las capacidades de sus empleados.

3 de cada 4
empresas encuestadas creen que la IA tendrá un impacto extremo o significativo en la tecnología de seguridad electrónica en los próximos 5 años.

El **36%**
de las empresas encuestadas ya utiliza el análisis basado en IA / aprendizaje automático.

El **41%**
de las que aún no lo utilizan, están interesadas en usarlo en los próximos 18 meses.

Datos procedentes de una encuesta externa realizada por Securitas Technology, en la que participaron 1.100 responsables de la toma de decisiones sobre seguridad y de la implantación de sistemas de seguridad de diferentes sectores en Australia, Francia, Alemania, Reino Unido y Estados Unidos.

Equilibrar la inteligencia artificial y la experiencia humana para impulsar la eficiencia de la seguridad

Potenciar la eficiencia humana con inteligencia artificial y análisis de datos

Supervisar la seguridad de una entidad comercial es un trabajo exigente. Las personas han soportado el peso de esta responsabilidad durante siglos, afrontando la gestión de numerosas medidas para proteger a las personas, los bienes y los activos. Ante la creciente necesidad de equilibrar el papel de las personas y de la tecnología, las empresas están explorando formas en que las tecnologías basadas en la IA puedan ayudar a aumentar la productividad y mejorar la eficiencia y el rendimiento de sus empleados.

Para los responsables de seguridad, la IA puede ser una herramienta poderosa capaz de utilizar los datos recopilados por sus sistemas de seguridad para generar valor operativo ahorrando tiempo y costes. A medida que se expande la adopción de la IA, también lo hace la oportunidad de que la gestión de la seguridad sea más eficiente. Por ejemplo, cuando se aplica a la videovigilancia, el software basado en la inteligencia artificial y en el análisis se puede utilizar para filtrar eficazmente actividades que no constituyen una amenaza y falsas alarmas que generan alertas innecesarias. Cada segundo de tiempo de una persona que esta tecnología permite ahorrar contribuye a crear un programa de seguridad más económico.

Pasar a la detección y prevención de amenazas

Tanto para las empresas como para los operadores de seguridad, visualizar horas de material de vídeo para revisar retrospectivamente las amenazas de seguridad no es ni productivo ni rentable. Gracias a la tecnología de IA generativa, esta forma tradicional de control de seguridad es cada vez menos utilizada, ya que las **empresas están empezando a utilizar la detección de anomalías y el análisis de vídeo inteligente para ayudar a distinguir las amenazas auténticas.** Estas plataformas de software pueden integrarse con sistemas de vídeo y configurarse para detectar anomalías como incendios, personas y vehículos no autorizados, animales, comportamientos inusuales como merodeo, seguimientos e incluso riesgos para la salud y la seguridad.

"La IA está llevando a nuestro sector hacia una seguridad proactiva frente a la seguridad tradicional reactiva. La IA Generativa tiene el potencial de cambiar aún más nuestra interacción con los sistemas, permitiéndonos utilizarlos de forma mucho más eficiente."

Doug Walsh | VP Global Technology Strategy | Securitas Technology

La IA Generativa está llamada a redefinir el control de videovigilancia permitiendo a los operadores de seguridad controlar los sistemas de manera conversacional y extraer información detallada bajo demanda o mediante alertas automatizadas. Por ejemplo, el sistema podría notificar a un operador una anomalía describiéndola con detalle en un lenguaje sencillo. De manera similar, el operador podría pedirle al sistema que responda preguntas de seguimiento para ayudar en la investigación. Gracias a que la IA Generativa ayuda a identificar de forma proactiva este tipo de escenarios, los seres humanos pueden tomar desde un primer momento medidas específicas para ayudar a prevenir que se produzcan posibles incidentes.

La importancia de mantener al ser humano informado

En la búsqueda de una sociedad más segura, el desarrollo de tecnología inteligente puede influir positivamente en la forma en que se gestiona la seguridad dentro de las empresas y con el público. **A medida que los sistemas electrónicos sean más inteligentes, también lo serán las personas responsables de administrarlos, tomando decisiones más inteligentes basadas en datos más extraordinarios.**

Las personas seguirán ocupando un papel central en todas las etapas del proceso de seguridad, desde el desarrollo de nuevas innovaciones basadas en la inteligencia artificial y el aprendizaje automático, hasta la construcción e instalación del hardware, su programación, la reacción a las alertas y, en última instancia, la respuesta física necesaria si se agrava una amenaza para la seguridad. El ojo humano ve las cosas de manera diferente. Y aunque los algoritmos de inteligencia artificial/aprendizaje automático pueden ayudarnos a identificar amenazas de forma más eficiente, las personas seguirán siendo las responsables de la decisión final.

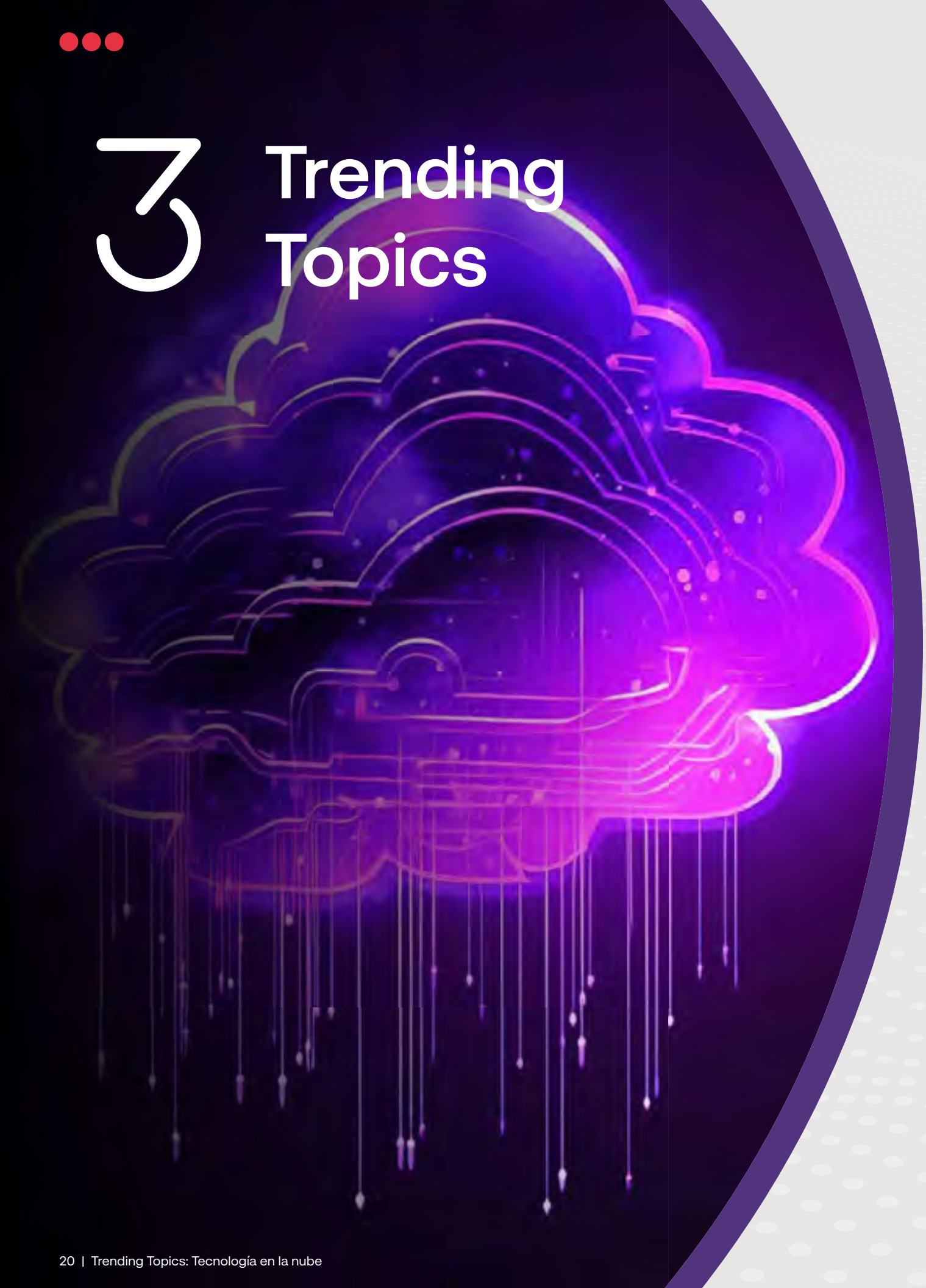
Visión de un futuro en el que la predicción impulse la prevención

¿Qué pasaría si la IA pudiese ayudar a predecir amenazas para la seguridad? Si bien aún faltan décadas para que logremos la Inteligencia Artificial General (IAG) o la Superinteligencia Artificial (SIA), esta es la apasionante posibilidad que tiene por delante el sector con la IA. Queda por ver hasta dónde llegará esto, pero con hardware cada vez mejor, más pequeño y menos costoso, y más sistemas migrando a la nube, la dirección que está tomando el sector es clara.

Pero con esta oportunidad viene la responsabilidad de cumplir con la nueva legislación que se está introduciendo para ayudar a regular el uso ético de la IA. En Europa, la Ley de IA de la UE clasifica los sistemas de IA con arreglo a sus posibles riesgos para las personas y en función de ello establece distintos grados de regulación. El uso de la biometría, regulado por el Parlamento Europeo en marzo de 2024, es un área sujeta a un mayor control con la introducción de esta ley.

Creemos que el futuro de la seguridad radica en encontrar el equilibrio entre lo humano y lo tecnológico. Si bien la IA puede aportar inteligencia avanzada e innovación al mundo de la seguridad corporativa, siempre será necesaria una intervención humana para actuar ante amenazas graves y adoptar medidas decisivas cuando sea necesario. Para liberar el potencial e impulsar el progreso, el sector de la seguridad debe adoptar la tecnología basada en la IA y cumplir con la legislación en evolución, manteniendo siempre informadas a las personas.

3 Trending Topics



Tecnología en la nube

Al igual que muchos mercados, el sector de la seguridad ha experimentado en los últimos años un rápido cambio hacia la tecnología basada en la nube.

Hoy en día, la aceleración del panorama de los servicios en la nube está llevando a los fabricantes de seguridad electrónica a desarrollar y optimizar sus productos y plataformas para satisfacer la demanda actual y futura de soluciones alojadas en la nube.

La migración a la nube se está convirtiendo en una prioridad cada vez más importante para las empresas preocupadas por la seguridad. Por ello, abordamos los temas e innovaciones principales sobre tecnología basada en la nube que surgirán en 2025 y durante los próximos años.

El **58%** ha implantado tecnología de seguridad basada en la nube.

Razones principales para su uso:

- Aumento de la protección en ciberseguridad
- Impulso de la eficiencia
- Facilidad de uso y gestión

La ciberseguridad y el cumplimiento de la legislación sobre protección de datos son las principales preocupaciones de las empresas que todavía no utilizan la tecnología de seguridad basada en la nube.

Datos procedentes de una encuesta externa realizada por Securitas Technology, en la que participaron 1.100 responsables de la toma de decisiones sobre seguridad y de la implantación de sistemas de seguridad de diferentes sectores en Australia, Francia, Alemania, Reino Unido y Estados Unidos.

Superando la brecha: generar confianza en la adopción de la seguridad en la nube

Centrarse en las funciones por encima de las características

La tecnología en la nube abre nuevas posibilidades en el mercado de la seguridad, brindando oportunidades y soluciones basadas en datos que aportan a los clientes una amplia gama de beneficios adicionales. Entre ellos se encuentran:

- Mayor escalabilidad y posibilidades de integración del sistema.
- Actualizaciones automáticas de software y firmware
- Acceso a análisis de datos sofisticados con inteligencia artificial (IA)
- Reparación remota, diagnóstico del estado del sistema y mantenimiento preventivo
- Gestión simplificada del sistema mediante aplicaciones móviles
- Modelos de pago flexibles basados en suscripciones
- Paso de CapEx a OpEx

Por lo general, los componentes del sistema, como cámaras, sensores y lectores de acceso, ofrecen atributos similares en todos los ámbitos. A medida que cada vez más clientes tienen en cuenta los beneficios de las soluciones basadas en la nube, la atención principal ha pasado ahora de la evaluación de los fabricantes individuales y de las características del producto a la funcionalidad global que ofrece una solución alojada en la nube. Además, la opción de pagar estas soluciones mediante una suscripción mensual ofrece a las empresas una alternativa rentable al gasto de capital inicial.

Cómo aprovechar el poder de los datos para liberar el potencial

Durante décadas, el almacenamiento de datos y la capacidad de procesamiento han sido las mayores barreras para la innovación en el sector de la seguridad. Las soluciones locales convencionales restringían la cantidad de datos de seguridad que podían manejar el hardware y los servidores in situ de los usuarios finales, lo que limitaba el almacenamiento de material de videovigilancia y las credenciales de control de accesos.

Actualmente, la evolución de la infraestructura en la nube ha abierto un mundo de oportunidades en toda la cadena de valor de la seguridad, liberando a los fabricantes de productos, desarrolladores de software y usuarios finales de los límites de procesamiento de datos que antes les impedían aprovechar todo el potencial de la tecnología.

"Las soluciones en la nube ofrecen tranquilidad a los usuarios. El usuario final ya no se tiene que ocupar a diario del mantenimiento de los servidores ni de las actualizaciones de software. Puede concentrarse en su propio trabajo y seguir utilizando sus sistemas, sin interrupciones."

Serdar Ince | VP Global Technology Innovation | Securitas Technology

Considerar y contrarrestar las preocupaciones sobre ciberseguridad

Si bien el interés por la tecnología en la nube sigue creciendo, las empresas siguen siendo cautelosas a la hora de gestionar sus sistemas de seguridad y datos dentro del espacio digital. La preocupación por la ciberseguridad es una de las principales razones por las que las empresas se resisten a migrar a soluciones en la nube, además de los costes de los equipos y el desconocimiento.

A medida que nuestro mundo está más conectado, las amenazas cibernéticas como los ataques de ransomware y las violaciones de datos serán siempre una preocupación legítima para las empresas. Esto hace que la necesidad de una estrategia integral de ciberseguridad sea tan importante como la implantación de un programa sólido de seguridad física.

Paradójicamente, resulta interesante que las empresas que ya han migrado a la nube (o tienen la intención de hacerlo) indican la necesidad de aumentar la protección en cuanto a ciberseguridad como su principal motivación para invertir en soluciones en la nube. A medida que más y más empresas dan el salto a la seguridad alojada en la nube, las que tienen reservas deben sopesar los riesgos y las beneficios de seguir sus pasos.

Para las empresas que comprensiblemente se muestran cautelosas a la hora de migrar todo su programa de seguridad a la nube, existe una opción tranquilizadora disponible para ayudar a cerrar la brecha entre las medidas de seguridad establecidas localmente y las soluciones de "nube real" completamente migradas. Se trata de modelos de "nube híbrida", donde los datos se almacenan principalmente en equipos locales, pero con una opción para enviar estos datos a un software alojado en la nube. Si bien la migración a una verdadera solución en la nube puede ser un proceso largo (como lo afirman los miembros de nuestro Consejo Asesor de Clientes que actualmente están en transición a verdaderas soluciones en la nube a través de modelos híbridos), las empresas pueden usar este tiempo para familiarizarse con los beneficios de la tecnología en la nube y las funciones avanzadas que ofrece.

La nube como nueva normalidad

Está claro que la seguridad basada en la nube pronto se convertirá en el enfoque estándar para la configuración de sistemas de seguridad y la gestión de datos. Si bien aún queda camino por recorrer antes de que este movimiento se adopte universalmente, la confianza en la nube está creciendo entre la comunidad empresarial, gracias a la educación continua del mercado, el desarrollo de la tecnología y la legislación que regula su uso.

Las empresas deben intensificar ahora sus preparativos para un futuro digital en el que los crecientes beneficios de la nube eclipsarán a las configuraciones tecnológicas tradicionales en las próximas décadas.

4 Trending Topics

Ciberseguridad y protección de datos

En el mundo actual interconectado, implantar una estrategia clara de ciberseguridad es esencial para que todas las empresas puedan aprovechar su red y experimentar los beneficios de la tecnología de seguridad electrónica avanzada.

Con más sistemas y dispositivos de seguridad que nunca conectados a redes de datos, la necesidad de mitigar las crecientes amenazas a la ciberseguridad y la protección de datos es cada vez mayor. Esta preocupación es compartida por los miembros de nuestro Consejo Asesor de Clientes, quienes señalan la ciberseguridad como un desafío prioritario tanto en el presente como en el futuro.

En este apartado, abordaremos las razones clave por las priorizar la ciberseguridad puede ayudar a las empresas a fortalecer su protección, garantizar el cumplimiento normativo y asegurar la continuidad operativa mediante su programa de seguridad electrónica.

1/3
de las empresas cuentan con procesos claros de ciberseguridad e higiene cibernética al evaluar las tecnologías de seguridad electrónica.

Uno de los 3 factores principales
que tienen en cuenta las empresas al elegir tecnologías de seguridad electrónica es la ciberseguridad.

Datos procedentes de una encuesta externa realizada por Securitas Technology, en la que participaron 1.100 responsables de la toma de decisiones sobre seguridad y de la implantación de sistemas de seguridad de diferentes sectores en Australia, Francia, Alemania, Reino Unido y Estados Unidos.

Asegurar los fundamentos: Un enfoque de tecnología de seguridad que priorice la ciberseguridad

La convergencia de la seguridad y la infraestructura de TI

Los sistemas de seguridad actuales aprovechan la infraestructura de TI con la que cuentan todas las empresas con visión de futuro: redes de datos, analítica de borde, servicios en la nube, inteligencia artificial (IA) y más. Atrás quedaron los días en los que la tecnología de seguridad podía gestionarse como algo separado y distinto de todas las demás tecnologías de las que dependen las empresas. Hoy en día, todo lo necesario para asegurar las redes TI debe aplicarse también a la infraestructura de seguridad electrónica.

La gravedad de las amenazas a la ciberseguridad puede variar, pero incluso la violación de la seguridad de los datos más pequeña puede generar rápidamente consecuencias catastróficas para las empresas. Dado que los sistemas de seguridad son una parte importante de la red de TI, adoptar un enfoque serio en la gestión de riesgos de seguridad cibernética, protección de datos e higiene cibernética continua es esencial para minimizar las innumerables amenazas procedentes de terceros maliciosos que tratan de acceder a datos intelectuales, personales y financieros a través de dispositivos conectados no seguros.

Las empresas deben aplicar a sus sistemas de seguridad las mismas buenas prácticas que utilizan para la ciberseguridad de las TI, como la gestión de usuarios y permisos, la protección de puntos finales y las actualizaciones continuas de software y firmware. Las empresas deben asegurarse de que se efectúe un mantenimiento preventivo regular de sus sistemas de seguridad electrónica y, al mismo tiempo, revisar las instalaciones heredadas que puedan requerir parches o actualizaciones para protegerlas contra posibles vulnerabilidades. **Llevar al día estas tareas ayudará a garantizar que los sistemas de seguridad se mantengan operativos en caso de ciberataque, una de las principales preocupaciones planteadas por nuestro Consejo Asesor de Clientes.**

Ahora más que nunca, mantener medidas de seguridad sólidas exige una estrecha colaboración entre los equipos de TI, seguridad y los responsables ejecutivos, como el CIO, además de una alianza estratégica con el proveedor de seguridad. Esto garantizará una mayor confianza en la ciberseguridad para todas las partes interesadas

Por qué la inteligencia de datos requiere mayor protección

Los sistemas de seguridad electrónica cada vez más conectados pueden aprovechar el poder de la nube para tratar más datos que nunca. Esta capacidad de "inteligencia de datos" permite a las empresas hacer más con sus sistemas de seguridad, desde aprovechar la IA y el análisis predictivo hasta administrar los sistemas de forma remota desde plataformas móviles centralizadas.

"Para cualquier empresa, proteger los datos confidenciales se ha vuelto tan importante como proteger a las personas, los bienes y los activos. Nuestros clientes se dan cuenta de que contar con una estrategia sólida de seguridad cibernética es fundamental para la integridad de su red de datos y de los sistemas de seguridad electrónica conectados a ella, especialmente a medida que más clientes se plantean dar el salto a soluciones de seguridad basadas en la nube."

Mike Beattie | CIO & SVP Information Global Technology | Securitas Technology

La sensibilidad de los datos de seguridad y la creciente necesidad de un almacenamiento seguro hacen que su protección sea más crucial que nunca. También hay que tener en cuenta que los sistemas de seguridad a menudo abarcan miles de dispositivos conectados, lo que los convierte en un objetivo potencial para piratas informáticos externos que intentan infiltrarse en la red. Afortunadamente, los fabricantes de productos de seguridad y los desarrolladores de software no dejan esto al azar. Prueba de ello es que las credenciales cibernéticas, la integridad de los datos y la conectividad remota se han convertido en factores clave en las decisiones de compra de seguridad electrónica por parte de los clientes.

Aunque el estado de los sistemas de seguridad basados en la red puede supervisarse de forma remota, la actualización del software central y del firmware de los dispositivos sigue siendo un proceso manual a cargo del proveedor de servicios para garantizar que los sistemas permanezcan actualizados y protegidos contra ciberamenazas.

Para minimizar el riesgo de que los sistemas ejecuten software desactualizado que pueda exponerlos a vulnerabilidades, las empresas pueden optar por soluciones en la nube y software como servicio (SaaS), que permiten la actualización automática del software y firmware en cuanto se lanzan nuevas versiones, asegurando así una protección continua.

Navegar por la normativa cambiante sobre ciberseguridad y protección de datos

El cumplimiento cibernético es ahora una consideración fundamental para las empresas que desean introducir tecnología de seguridad avanzada en su programa de seguridad. La legislación sobre ciberseguridad y protección de datos puede variar de un país a otro, por lo que es esencial que los responsables de seguridad conozcan las normas locales sobre tratamiento de datos y uso de datos del sistema de seguridad antes de realizar cualquier inversión.

Sin embargo, tanto en la Unión Europea como en Estados Unidos existe un marco claro para trabajar.

Por ejemplo, en Europa, la Directiva sobre redes y sistemas de información (NIS) [1] es la primera norma obligatoria sobre ciberseguridad dirigida a empresas y proveedores que prestan servicios esenciales o importantes. Esta norma ha sido revisada para tener en cuenta la digitalización ampliada y las amenazas a la seguridad, en la llamada NIS2. En Estados Unidos, el Instituto Nacional de Estándares y Tecnología (NIST) [2] ofrece orientación a las empresas a través de su Marco de Ciberseguridad (CSF) 2.0. Si bien actualmente el CSF es obligatorio únicamente para las agencias

del Gobierno Federal de EE. UU., se anima a todas las empresas a seguir las directrices proporcionadas por el CSF y aplicar las mejores prácticas.

Las empresas también pueden tomar medidas proactivas más allá del cumplimiento de estas normas para identificar y mitigar los riesgos de ciberseguridad y protección de datos. Consultar con un proveedor de seguridad especializado como Securitas ayudará a las empresas a estar al día con los cambios y a tomar decisiones informadas sobre cómo:

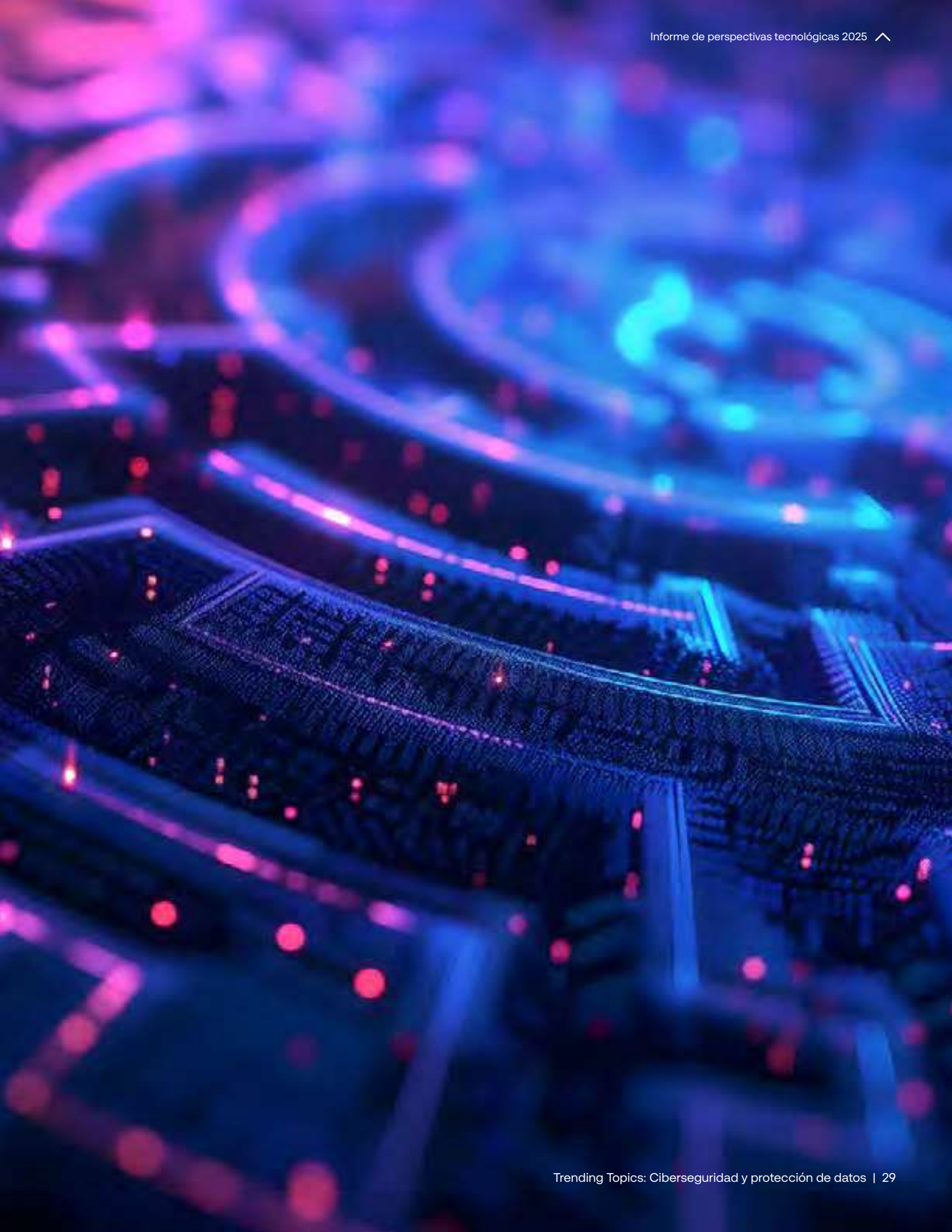
- Proteger eficazmente tu empresa contra los riesgos de ciberseguridad.
- Incorporar con confianza tecnologías de futuro en tu estrategia de seguridad empresarial.
- Responder a las expectativas crecientes de ciberseguridad de los clientes y la cadena de suministro.

Además, nuestros socios tecnológicos estratégicos analizan muchos aspectos prácticos de ciberseguridad en este informe.

Afrontar el futuro con la mente puesta en el espacio cibernético

La tendencia en materia de ciberseguridad y protección de datos seguirá siendo un tema clave en el sector de la seguridad. Si afrontan el futuro considerando prioritarios los aspectos cibernéticos, con el respaldo de una base concreta de ciberseguridad, las empresas se colocarán en la mejor posición posible para mitigar y minimizar eficazmente los riesgos cibernéticos y de protección de datos.

Referencias:
[1] https://digital-strategy.ec.europa.eu/en/policies/nis2-directive
[2] https://www.nist.gov/cyberframework



5 Trending Topics

Sostenibilidad

¿El uso de tecnología de seguridad puede ayudar a las empresas a alcanzar sus objetivos de sostenibilidad?

Esta es la importante pregunta que se plantea cada vez con más frecuencia en relación con la cadena de suministro de seguridad electrónica, a medida que las empresas de todo el mundo buscan formas más sostenibles de trabajar y hacer negocios.

También es el tema central de este apartado, que considera la sostenibilidad como un tema de actualidad dentro del mundo de la tecnología de seguridad y analiza la forma en la que el sector está asumiendo la responsabilidad de ofrecer soluciones y servicios más sostenibles.

Más de la mitad
de las empresas ya utilizan soluciones de seguridad electrónica para contribuir a reducir el impacto medioambiental y los costes operativos.

El **35%**
de las empresas está estudiando activamente formas de integrar la sostenibilidad en sus sistemas de seguridad.

3 de cada 4
empresas quiere saber más sobre cómo pueden utilizar sus tecnologías de seguridad para contribuir a alcanzar sus objetivos de sostenibilidad.

Datos procedentes de una encuesta externa realizada por Securitas Technology, en la que participaron 1.100 responsables de la toma de decisiones sobre seguridad y de la implantación de sistemas de seguridad de diferentes sectores en Australia, Francia, Alemania, Reino Unido y Estados Unidos.

Adopción de la sostenibilidad en el sector de la seguridad electrónica

Creación de una cultura de sostenibilidad en toda la cadena de suministro

Para asegurar un futuro sostenible para nuestro planeta, todas las empresas deben asumir la responsabilidad de reducir su impacto en el medio ambiente. Se trata de una tarea compartida por toda la cadena de suministro de seguridad, desde los fabricantes de tecnología y los integradores hasta los propios usuarios finales. Sin lugar a dudas, la necesidad mundial de hacer frente al cambio climático se ha convertido en un problema urgente y las empresas de todo tipo deberían tomar medidas proactivas para minimizar su huella ambiental, incluida la inversión en nuevos procesos y tecnologías para avanzar en su camino hacia la descarbonización y la sostenibilidad.

Para los responsables de abastecimiento, la huella ambiental de los productos y servicios se ha convertido en un factor importante en sus decisiones de compra comercial, también cuando se trata de adquirir tecnología de seguridad. Deben sopesar en qué medida afectarán sus decisiones tecnológicas a los objetivos de sostenibilidad internos y los requisitos de responsabilidad social corporativa basados en los Objetivos de Desarrollo Sostenible (ODS) de Naciones Unidas y la iniciativa de Objetivos Basados en la Ciencia (SBTi). Por supuesto, la búsqueda de opciones sostenibles se hace más fácil cuando se pueden conocer con facilidad las credenciales ambientales de los productos, soluciones y proveedores de servicios.

Quizás el papel más destacado es el de los fabricantes de tecnología de seguridad. Estas empresas serán fundamentales para reforzar la atención sobre la sostenibilidad dentro de la cadena de suministro de seguridad más amplia en los próximos años. Desde el abastecimiento ético de materiales y la fabricación de hardware hasta el embalaje y la distribución de productos, cada eslabón de esta parte de la cadena de suministro tiene un impacto directo o indirecto en el medio ambiente. Por consiguiente, la necesidad de medir la magnitud de este impacto está adquiriendo importancia intrínseca, y los integradores y los usuarios finales tienden a considerar las credenciales de sostenibilidad al tomar sus decisiones de inversión.

En términos positivos, ahora hay más proveedores que dan prioridad al desarrollo de productos energéticamente eficientes y muestran sus esfuerzos de sostenibilidad dentro de sus propuestas de valor. Hasta hace poco, esta información era menos visible, pero para dar respuesta al aumento de los costes de la energía y a la urgente necesidad de soluciones más ecológicas, los proveedores están avanzando para comunicar claramente los factores ambientales, sociales y de gobernanza (ESG) a los clientes. Esto incluye el cálculo y la visualización de datos sobre el consumo de energía y los factores de emisión (FE) para mostrar la huella de carbono de los diferentes productos y soluciones.

Afrontar los retos de la sostenibilidad con tecnología

La inteligencia y la innovación en la tecnología de seguridad han dado lugar a nuevas formas de aprovechar los datos del sistema para algo más que la protección. Más allá de la seguridad, las empresas utilizan sus sistemas para mejorar la eficiencia operativa y supervisar la salud y la seguridad de los empleados. De la misma manera, las tecnologías de seguridad como la videovigilancia y el control de accesos también pueden utilizarse para ayudar a las empresas a ser sostenibles.

A continuación se indican varios usos posibles que así lo demuestran:

Reducción de los desplazamientos de vehículos gracias a la conectividad remota

El acceso remoto a los sistemas de seguridad ofrece muchos beneficios de conveniencia y sostenibilidad. Por ejemplo, la posibilidad de que los clientes puedan ver y controlar sus sistemas de seguridad a través de aplicaciones móviles hace que sea mucho más fácil obtener una visión completa de su programa de seguridad en movimiento. Y para los proveedores de servicios, conectarse a los sistemas de los clientes de forma remota permite realizar operaciones de mantenimiento y reparaciones de los sistemas de forma más rápida y eficiente. Es fundamental, desde el punto de vista de la sostenibilidad, que cada oportunidad de reducir las emisiones de gases de efecto invernadero (GEI) suponga una diferencia positiva. Por lo tanto, el simple hecho de que se necesiten menos desplazamientos de vehículos y visitas físicas in situ significa que se puede ahorrar energía valiosa.

Optar por alternativas de bajas emisiones

A medida que la sostenibilidad gana protagonismo en la industria de la seguridad, los clientes tendrán acceso a información más detallada sobre el impacto ambiental de los productos y soluciones que utilizan.

Los fabricantes están incorporando estos datos en fichas técnicas y Declaraciones Ambientales de Producto (EPD), documentos clave que reflejan la huella de carbono a lo largo del ciclo de vida de cada producto.

Este nivel de transparencia no solo permite tomar decisiones más informadas, sino que también ayuda a las empresas a alinear sus estrategias de seguridad con sus objetivos de sostenibilidad, reduciendo su impacto ambiental sin comprometer la protección y el rendimiento tecnológico.

Actuar a partir de datos de aforo y análisis de vídeo

Los administradores de instalaciones confían en los datos para administrar y optimizar sus edificios. Los datos de aforo procesados por la tecnología de control de accesos y videovigilancia pueden ofrecer información útil para conocer las áreas de un edificio que tienen el nivel más alto o más bajo de ocupación y cuándo.

Por ejemplo, los sistemas de control de accesos capturan datos cada vez que una persona accede a una puerta, entra en un área o sale de un edificio. Las tendencias de estos datos a lo largo del tiempo pueden ayudar a los administradores de edificios a reconocer patrones de flujo de personas y conocer los momentos en los que habitualmente los edificios y zonas específicas se utilizan poco o están desocupados.

Los sistemas de vídeo con software de análisis de datos integrado (en el borde) o basado en la nube permiten que las cámaras capturen mucho más que solo imágenes de seguridad y realicen, por ejemplo, el recuento de personas. En este caso, se pueden utilizar cámaras situadas estratégicamente para hacer un seguimiento de la afluencia contando el número de personas que entran y salen de un edificio, piso o sala específicos. Esto proporciona a los administradores de seguridad información sobre el número de personas que se encuentran en un área en tiempo real y en períodos más largos.

Estos dos ejemplos podrían ayudar a justificar las decisiones de apagar los sistemas de iluminación, calefacción, ventilación y aire acondicionado (HVAC) en los momentos de baja o nula ocupación, lo que ayudaría a reducir el consumo innecesario de energía y a ahorrar energía valiosa.

Además de la necesidad de que todas las empresas contribuyan a los objetivos mundiales de desarrollo sostenible, la sostenibilidad es un tema crucial que el sector de la seguridad debe adoptar plenamente. Todas las partes interesadas involucradas en el sector, incluidos fabricantes, desarrolladores de software, distribuidores, instaladores, integradores y proveedores de servicios, pueden desempeñar un papel fundamental en el fomento de la sostenibilidad. El énfasis en la innovación dentro de la cadena de suministro puede conducir al descubrimiento de más oportunidades para destacar cómo la tecnología de seguridad puede ofrecer valor a los clientes y contribuir a sus esfuerzos de sostenibilidad.

"Así como cada cliente tiene necesidades de seguridad únicas, también tiene objetivos de sostenibilidad específicos. Si conocemos a fondo estos desafíos desde el principio, podemos trabajar en colaboración con los clientes para ofrecer soluciones de seguridad más sostenibles que contribuyan positivamente a los objetivos de sostenibilidad compartidos.

Hay muchos factores a tener en cuenta al buscar soluciones de seguridad sostenibles, incluida la eficiencia energética de los productos y el potencial de aprovechar información basada en datos para optimizar el uso de los edificios. Como punto de partida, las empresas deben dar prioridad a los socios que demuestren claramente su compromiso con la sostenibilidad y la innovación en su oferta."

John Tomin | Global Sustainability Officer | Securitas Technology

Securitas España
900 907 207
info@securitas.es

securitas.es